

ALLTEL CORPORATION

601 Pennsylvania Avenue, N.W.
Suite 720
Washington, DC 20004
202-783-3970
202-783-3982 fax



February 29, 2008

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Suite TW-A325
Washington, D.C. 20554

In Re: Alltel Communications, LLC
(FRN No. 0017176645)
CPNI Certifications Pursuant to
47 C.F.R. Sec. 64.2009(e)
EB Docket No. 06-36

Via Electronic Filing

Dear Ms. Dortch:

Alltel Communications, LLC. ("Alltel"), the successor in interest to Alltel Communications, Inc., transmits herewith on behalf of itself, its wholly owned licensee subsidiaries and controlled licensee affiliates, its annual certifications for calendar year 2007 regarding the use and protection of Customer Proprietary Network Information ("CPNI") as required by Section 64.2009(e) of the Commission's rules.

Please address any questions regarding this transmittal to undersigned counsel either at the above-address or at (202) 783-3976.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Glenn S. Rabin", written over the typed name.

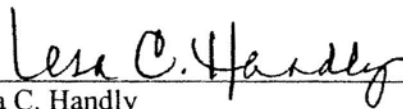
Glenn S. Rabin
Vice President
Federal Communications Counsel
Alltel Communications, LLC

Attachments

CC: Enforcement Bureau, FCC
Best Copy and Printing, Inc.

ALLTEL COMMUNICATIONS, LLC
ANNUAL SECTION 64.2009(e) CERTIFICATION

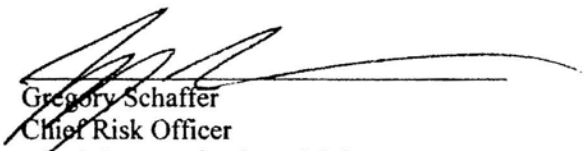
I, Lesa C. Handly, a duly authorized officer of Alltel Communications, LLC ("Alltel") hereby certify on behalf of Alltel that I have personal knowledge that Alltel has operating procedures, as described in sections A through C of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION, ("Statement") that, to the best of my knowledge, information and belief, are adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.



Lesa C. Handly
Senior Vice President -
Customer Strategies
Alltel Communications, LLC
February 17, 2008

**ALLTEL COMMUNICATIONS, LLC
ANNUAL SECTION 64.2009(e) CERTIFICATION**

I, Gregory Schaffer, a duly authorized officer of Alltel Communications, LLC ("Alltel") hereby certify on behalf of Alltel that I have personal knowledge that Alltel has operating procedures, as described in sections D through G of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("Statement"), that, to the best of my knowledge, information and belief, are adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.


Gregory Schaffer
Chief Risk Officer
Alltel Communications, LLC
February 29, 2008

**STATEMENT OF OPERATING PROCEDURES IMPLEMENTING
47 C.F.R. SUBPART U GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION
FOR THE PERIOD JANUARY 1, 2007 TO DECEMBER 7, 2007**

The following explains how the operating procedures of Alltel Communications, LLC (formerly Alltel Communications, Inc., and collectively "Alltel")¹ ensures that it is in compliance with the Commission's CPNI rules, as referenced herein and set forth in 47 C.F.R. Subpart U.

A. CPNI Use and Customer Approval

In accordance with 47 CFR 64.2005(a), Alltel uses CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer subscribes from Alltel. Alltel presently offers CMRS and information services. Consistent with 47 CFR 64.2005(b), Alltel does not use, disclose, or permit access to CPNI to market telecommunication service offerings outside the category of service to which the customer subscribes. Alltel uses CPNI derived from the provision of its CMRS services for the provision of CPE and information services. Alltel has not solicited customer consent to use CPNI in a manner that is beyond the existing service relationship and Alltel does not consider its customer's to have granted approval for such CPNI use. As a result, the requirements contained in the revised section 64.2007(b) (Use of Opt-Out and Opt-In Approval Processes) pertaining to the approval process applicable to using customer's individually identifiable CPNI for marketing communications-related services to such customers do not apply to Alltel's current operational use of CPNI. Alltel has a CPNI Marketing Policy which defines how CPNI may be used to market and provide services to Alltel customers. In accordance with that policy, Alltel requires that CPNI be used only for the purposes identified herein and as otherwise permitted.

B. Sales and Marketing Campaigns

Pursuant to 47 CFR 64.2009(a), Alltel reviews sales and marketing campaigns that use CPNI. All such campaigns are conducted to market services within the category of service the customer subscribes from Alltel in accordance with 47 CFR 64.2005(a). Alltel does not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Alltel has a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Alltel restricts the ability to create marketing campaigns in order to ensure compliance with the CPNI rules. The persons with authority to approve campaigns which use CPNI are at a minimum Director level employees.

Consistent with 47 CFR 2009(c), Alltel maintains records of the campaigns which use CPNI that are conducted by authorized personnel. Alltel's Privacy Office conducts

¹ Alltel Communications, Inc. converted from a Delaware corporation to a Delaware limited liability company effective December 31, 2007.

quarterly reviews of such campaign records to verify compliance with CPNI rules and Alltel policies. These records contain a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. This information is retained for at least one year. The results of the quarterly reviews are also analyzed by the Privacy Office and Legal staff to verify compliance with CPNI rules.

C. Training and Disciplinary Process

Alltel employees who are authorized to conduct marketing campaigns are trained to keep customer data strictly confidential. Alltel's Privacy Office conducts periodic CPNI education for personnel who are authorized to conduct campaigns as required by 47 CFR 64.2009(b). Specifically, such personnel are instructed as to the proper access and use of CPNI. Each person authorized to conduct a marketing campaign utilizing CPNI received this education in 2007.

Alltel's CPNI Marketing Policy expressly establishes a disciplinary process applicable to employees in the event it is determined that such policy has been violated. A violation of such policy subjects the employee to disciplinary action, up to and including termination.

D. Security Governance

Alltel has established an "Enterprise Information Security Program" (EISP) designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by the Company. Pursuant to the EISP Alltel maintains a Security Steering Committee that includes (among others) the Chief Operating Officer, the General Counsel, the Chief Financial Officer, the Executive Vice President for Network Services and the Senior Vice Presidents of Human Resources and IT Services. Alltel's Chief Risk Officer is responsible for an Enterprise Security and Risk Office that develops, implements and enforces security and privacy policies on a company wide basis.

E. Billing Records, Network Records, and Information

Alltel maintains billing detail data, call detail data, and network record data in applications secured by networks, systems, policies and processes designed to control, monitor, and limit access to authorized users with legitimate business needs.

Internal governance processes dictate that newly created applications and significant changes to existing applications that process or store customer data must be formally reviewed and analyzed by appropriate security and privacy teams. Alltel's Enterprise Security and Risk team reviews new applications and enhancements for compliance with existing security and privacy policies, which include requirements for access and authentication controls. Alltel's Internal Audit Department routinely reviews applications to test for compliance with existing security procedures.

F. Data Centers

All data centers have processes and procedures in place for controlling physical access into the data centers along with controlling system access. Compliance with security policies are reviewed by the Enterprise Security and Risk team and Internal Audit on a recurring basis.

G. Safeguards on the Disclosure of CPNI

Alltel's account verification policy establishes the circumstances and limitations under which Alltel call center and retail employees are allowed to disclose CPNI. These employees are monitored and rated for compliance with Alltel's account verification procedures.

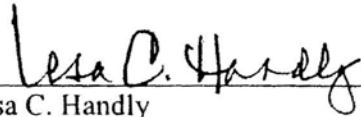
Alltel employees are trained to keep sensitive customer data strictly confidential and suspected breaches of customer confidentiality are investigated by corporate security teams. In addition to investigating reported incidents, security teams periodically conduct reviews of various systems to identify potential unauthorized access to customer data. Alltel requires newly-hired employees to sign an "Employee Agreement on Non-Disclosure and Non-Solicitation," which prohibits employees from disclosing information that is confidential to any third party. Confirmed unauthorized disclosures of customer information are subject to discipline, up to and including termination and referrals to law enforcement authorities where deemed appropriate.

Policies, practices and technologies are used to limit employee access to customer records on a business need basis. Initial access to a number of applications is controlled via an internal application that uses role-based logic and employee job requirements, as defined by the designated business owners, to limit access based on job function. Access to relevant financial reporting applications are reviewed quarterly by the designated business owner for Sarbanes-Oxley compliance. Quarterly reviews are also conducted of certain other applications containing sensitive customer or company data.

Alltel's privacy policy describes how Alltel uses, maintains and protects customer information, including CPNI. This policy is available to all customers and is available at www.alltel.com by clicking on 'Privacy Statement' at the bottom of the home page. In addition, Alltel's contracts with independent contractors that have access to confidential customer data are required to contain safeguards necessary to protect that data.

ALLTEL COMMUNICATIONS, LLC
ANNUAL SECTION 64.2009(e) CERTIFICATION

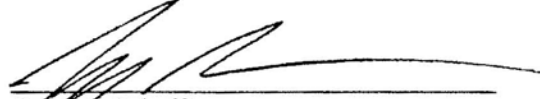
I, Lesa C. Handly, a duly authorized officer of Alltel Communications, LLC ("Alltel") hereby certify on behalf of Alltel that I have personal knowledge that Alltel has operating procedures, as described in sections A through C of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION, ("Statement") that, to the best of my knowledge, information and belief, are adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.



Lesa C. Handly
Senior Vice President -
Customer Strategies
Alltel Communications, LLC
February 27, 2008

**ALLTEL COMMUNICATIONS, LLC
ANNUAL SECTION 64.2009(e) CERTIFICATION**

I, Gregory Schaffer, a duly authorized officer of Alltel Communications, LLC ("Alltel") hereby certify on behalf of Alltel that I have personal knowledge that Alltel has operating procedures, as described in sections D through J of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("Statement"), that, to the best of my knowledge, information and belief, are adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.



Gregory Schaffer
Chief Risk Officer
Alltel Communications, LLC

February 29, 2008

**STATEMENT OF OPERATING PROCEDURES IMPLEMENTING
47 C.F.R. SUBPART U GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION
FOR THE PERIOD DECEMBER 8, 2007 TO DECEMBER 31, 2007**

The following explains how the operating procedures of Alltel Communications, LLC (formerly Alltel Communications, Inc., and collectively "Alltel")¹ ensures that it is in compliance with the Commission's CPNI rules, as referenced herein and set forth in 47 C.F.R. Subpart U.

A. CPNI Use and Customer Approval

In accordance with 47 CFR 64.2005(a), Alltel uses CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer subscribes from Alltel. Alltel presently offers CMRS and information services. Consistent with 47 CFR 64.2005(b), Alltel does not use, disclose, or permit access to CPNI to market telecommunication service offerings outside the category of service to which the customer subscribes. Alltel uses CPNI derived from the provision of its CMRS services for the provision of CPE and information services. Alltel has not solicited customer consent to use CPNI in a manner that is beyond the existing service relationship and Alltel does not consider its customer's to have granted approval for such CPNI use. As a result, the requirements contained in the revised section 64.2007(b) (Use of Opt-Out and Opt-In Approval Processes) pertaining to the approval process applicable to using customer's individually identifiable CPNI for marketing communications-related services to such customers do not apply to Alltel's current operational use of CPNI. Alltel has a CPNI Marketing Policy which defines how CPNI may be used to market and provide services to Alltel customers. In accordance with that policy, Alltel requires that CPNI be used only for the purposes identified herein and as otherwise permitted.

B. Sales and Marketing Campaigns

Pursuant to 47 CFR 64.2009(a), Alltel reviews sales and marketing campaigns that use CPNI. All such campaigns are conducted to market services within the category of service the customer subscribes from Alltel in accordance with 47 CFR 64.2005(a). Alltel does not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Alltel has a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Alltel restricts the ability to create marketing campaigns in order to ensure compliance with the CPNI rules. The persons with authority to approve campaigns which use CPNI are at a minimum Director level employees.

Consistent with 47 CFR 2009(c), Alltel maintains records of the campaigns which use CPNI that are conducted by authorized personnel. Alltel's Privacy Office conducts

¹ Alltel Communications, Inc. converted from a Delaware corporation to a Delaware limited liability company effective December 31, 2007.

quarterly reviews of such campaign records to verify compliance with CPNI rules and Alltel policies. These records contain a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. This information is retained for at least one year. The results of the quarterly reviews are also analyzed by the Privacy Office and Legal staff to verify compliance with CPNI rules.

C. Training and Disciplinary Process

Alltel employees who are authorized to conduct marketing campaigns are trained to keep customer data strictly confidential. Alltel's Privacy Office conducts periodic CPNI education for personnel who are authorized to conduct campaigns as required by 47 CFR 64.2009(b). Specifically, such personnel are instructed as to the proper access and use of CPNI. Each person authorized to conduct a marketing campaign utilizing CPNI received this education in 2007.

Alltel's CPNI Marketing Policy expressly establishes a disciplinary process applicable to employees in the event it is determined that such policy has been violated. A violation of such policy subjects the employee to disciplinary action, up to and including termination.

D. Security Governance

Alltel has established an "Enterprise Information Security Program" (EISP) designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by the Company. Pursuant to the EISP Alltel maintains a Security Steering Committee that includes (among others) the Chief Operating Officer, the General Counsel, the Chief Financial Officer, the Executive Vice President for Network Services and the Senior Vice Presidents of Human Resources and IT Services. Alltel's Chief Risk Officer is responsible for an Enterprise Security and Risk Office that develops, implements and enforces security and privacy policies on a company wide basis.

E. Billing Records, Network Records, and Information

Alltel maintains billing detail data, call detail data, and network record data in applications secured by networks, systems, policies and processes designed to control, monitor, and limit access to authorized users with legitimate business needs.

Internal governance processes dictate that newly created applications and significant changes to existing applications that process or store customer data must be formally reviewed and analyzed by appropriate security and privacy teams. Alltel's Enterprise Security and Risk team reviews new applications and enhancements for compliance with existing security and privacy policies, which include requirements for access and authentication controls. Alltel's Internal Audit Department routinely reviews applications to test for compliance with existing security procedures.

F. Data Centers

All data centers have processes and procedures in place for controlling physical access into the data centers along with controlling system access. Compliance with security policies are reviewed by the Enterprise Security and Risk team and Internal Audit on a recurring basis.

G. Safeguards on the Disclosure of CPNI

(1) Safeguarding CPNI

Alltel's account verification policy establishes the circumstances and limitations under which Alltel call center and retail employees are allowed to disclose CPNI. These employees are monitored and rated for compliance with Alltel's account verification procedures.

Alltel employees are trained to keep sensitive customer data strictly confidential and suspected breaches of customer confidentiality are investigated by corporate security teams. In addition to investigating reported incidents, security teams periodically conduct reviews of various systems to identify potential unauthorized access to customer data. Alltel requires newly-hired employees to sign an "Employee Agreement on Non-Disclosure and Non-Solicitation," which prohibits employees from disclosing information that is confidential to any third party. Confirmed unauthorized disclosures of customer information are subject to discipline, up to and including termination and referrals to law enforcement authorities where deemed appropriate.

Policies, practices and technologies are used to limit employee access to customer records on a business need basis. Initial access to a number of applications is controlled via an internal application that uses role-based logic and employee job requirements, as defined by the designated business owners, to limit access based on job function. Access to relevant financial reporting applications are reviewed quarterly by the designated business owner for Sarbanes-Oxley compliance. Quarterly reviews are also conducted of certain other applications containing sensitive customer or company data.

Alltel's privacy policy describes how Alltel uses, maintains and protects customer information, including CPNI. This policy is available to all customers and is available at www.alltel.com by clicking on 'Privacy Statement' at the bottom of the home page. In addition, Alltel's contracts with independent contractors that have access to confidential customer data are required to contain safeguards necessary to protect that data.

(2) Telephone Access to CPNI

By policy, reinforced with training and monitoring, Alltel customer service representatives are prohibited from disclosing call detail (as defined in 47 CFR 64.2003(d)) over the telephone. A customer service representative is allowed to assist the

customer in the event an authenticated customer first identifies the call to the representative without assistance during a call initiated by the customer. Upon request, Alltel will mail a copy of call detail to the customer's address of record. In the event a customer's address of record has changed in the thirty days prior to the telephone request, Alltel does not mail the requested call detail. Instead, Alltel advises such customers to utilize online or in-store access. Alltel policy does not permit faxing of call detail.

(3) Online Access to CPNI

Alltel maintains an online account retrieval system called "My Account" whereby Alltel customers may register their account and subsequently login to access their account information and CPNI only after providing a valid password. Prior to the relevant time period, Alltel had established operating procedures adequate to ensure compliance with the newly enacted CPNI rules relating to online access to CPNI, including a requirement that all customers who register for My Account receive a text message to the designated handset on the account being registered. Pursuant to these procedures, a code in the text message would be required to complete the registration process. All of the established procedures described herein were fully implemented prior to the relevant time period except the registration text message delivery to post paid customers, which was fully implemented on February 17, 2008.

Alltel customers who want online access to their account information and CPNI must first register their account on My Account. Prior to beginning the registration process, customers are required to provide Alltel their account number and mobile number. The post paid registration process requires customers to: (1) provide their name; (2) create a unique user identification; (3) create a password; and, (4) provide their electronic mail address.

My Account registration for Alltel business customers requires two data elements in addition to the My Account registration process for post paid consumers. Business customers are required to provide their business' tax identification number to Alltel and must create a personal identification number (PIN) after they have entered their user identification and password. For on-line access to CPNI after the registration for a business account is complete, users must submit their user identification, password and PIN.

Alltel prepaid customers register for online access to CPNI in the same manner as described above. Prepaid customers are sent a text message containing a unique code to their handset which is then used to complete the My Account registration process. Thereafter, prepaid customers must utilize their user identification and password for online access to CPNI.

Additionally, Alltel provides all customers the ability to block online access to their account and CPNI.

(4) Establishment of a Password and Back-Up Authentication Methods for Lost or Forgotten Passwords.

Alltel has made available a backup authentication method for customers who have forgotten their My Account password. This backup authentication method does not prompt the customer for readily available biographical or account information. If the customer does not provide the correct response for the backup authentication method, the customer is sent a code via text message to their handset. The customer is required to provide this code to Alltel prior to establishing a new password.

(5) Notification of Account Changes

Alltel immediately notifies customers via United States mail to their address of record, when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. Alltel does not reveal the changed information.

(6) In-Store Access to CPNI

Alltel requires customers to present valid photo identification and verifies the identity matches the account information prior to disclosing CPNI at an Alltel retail location and at Alltel agent retail locations.

H. Notification of CPNI Security Breaches

Alltel has enhanced existing processes in order to comply with the CPNI rules. Regular recurring meetings are conducted among Alltel's Enterprise Security and Risk Office and Legal staff to consider the current internal investigations involving potential CPNI breaches. Alltel reports confirmed CPNI breaches and notifies customers in accordance with the CPNI breach notification rules.

I. Summary of Customer Complaints Regarding the Unauthorized Release of CPNI

During the relevant period Alltel received four complaints from customers regarding the unauthorized release of CPNI. Alltel's Enterprise Security and Risk Office investigated these complaints and one of them did not appear to result in improper access to or unauthorized release of CPNI. There were three instances of apparent improper access and improper disclosure by employees to unauthorized individuals.

J. Action Taken Against Data Brokers

During the relevant period, Alltel has not initiated any actions against data brokers.